# Mac OS X Server In Depth

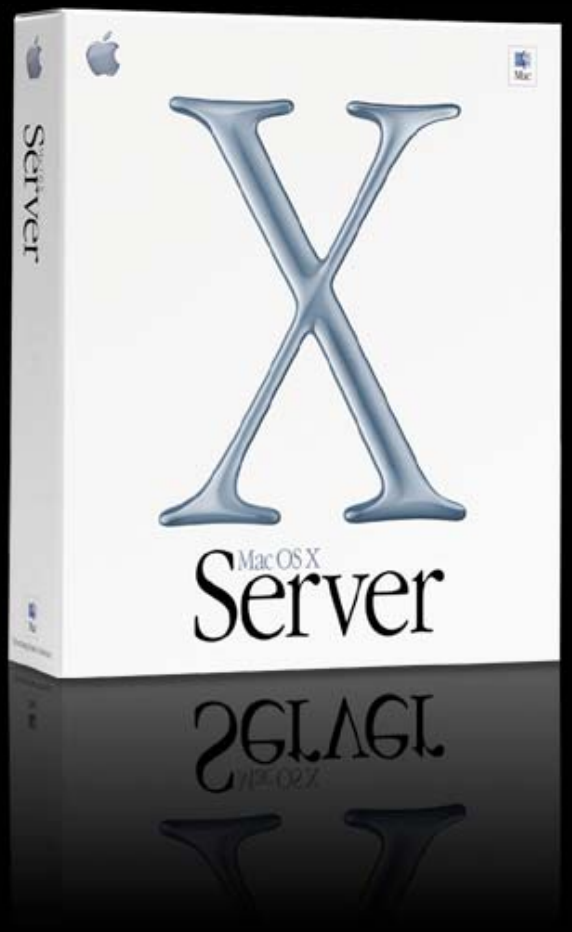
## Session 802

# Mac OS X Server In Depth

**Kazu Yanagihara**
**Manager, Core Server Development**

# Introduction

- Remote server administration and monitoring
- Open Directory
- High Availability Services
- File services update
- Web platform
- Q&A



# What You Will Learn

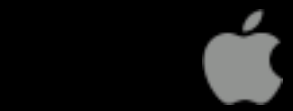
- How to design a remote server friendly software
- Key new platform capabilities of Jaguar Server
- What's new in file services area
- Where can I learn more?


Remote Server Administration
and Monitoring

# Remote Server Administration

**Server customers want…**

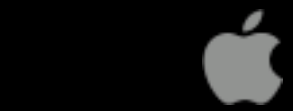
- Ability to boot server boxes without monitor
  - Save space
  - Save $$$
- Manage servers remotely
  - May be kept in secure server closet
  - Manage from anywhere—office, home, on the road . . .
- Monitor multiple servers remotely



# Remote Server Administration

## Jaguar Server enhancements

- Jaguar Server will support booting without monitor
- All management software will be remote friendly
  - Server Admin: Print Service module
  - Directory Setup
  - NetInfo Domain Setup
- Remote setting of key system preferences
- Remote software update



# Remote Server Administration

## Keep in mind…

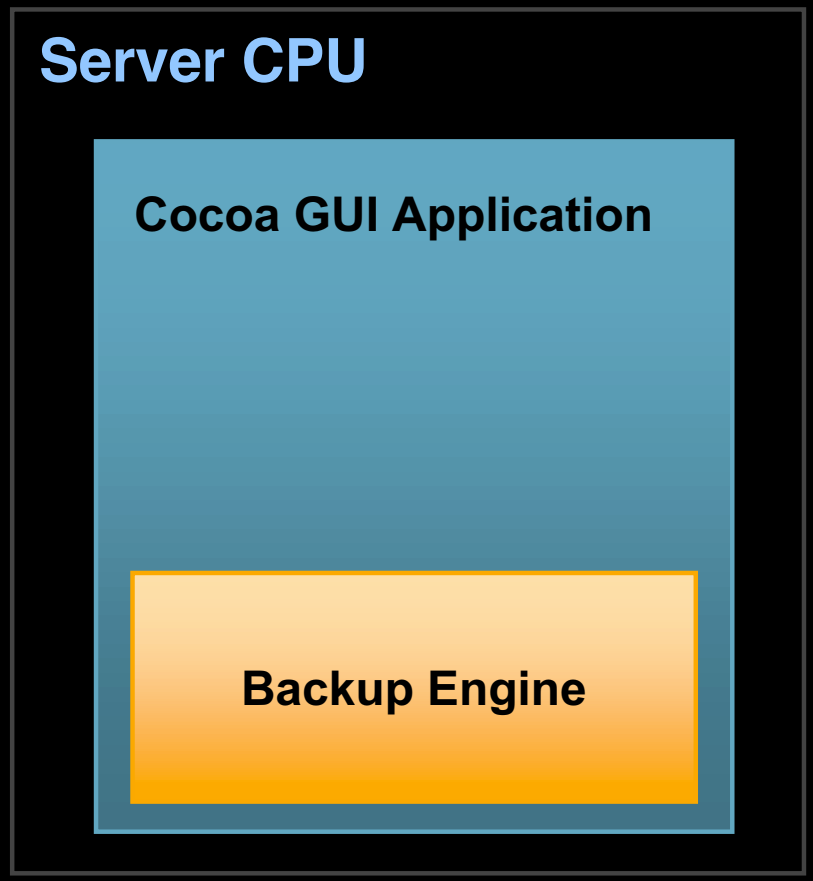
- Server may not have a monitor and keyboard attached
- Likely, there is no system login session
- Not all system services are available:
  - Finder
  - AppleScript
  - . . .

# Remote Server Administration

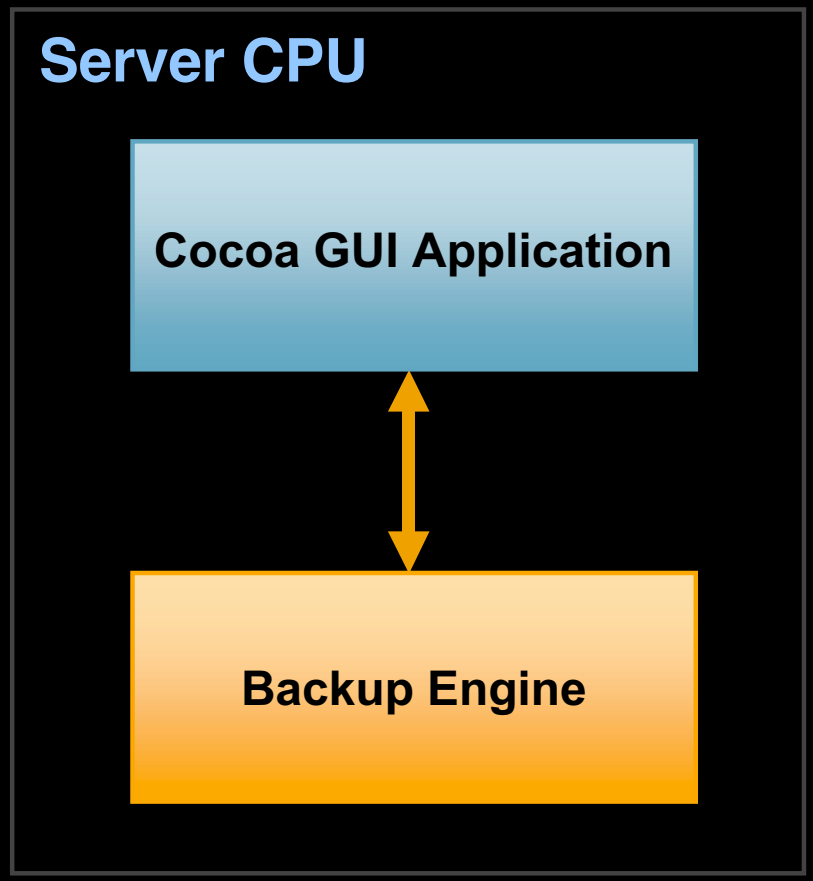
## What do server developers need to do?

- De-couple GUI from core functionality
- GUI component needs to be able to run locally or remotely

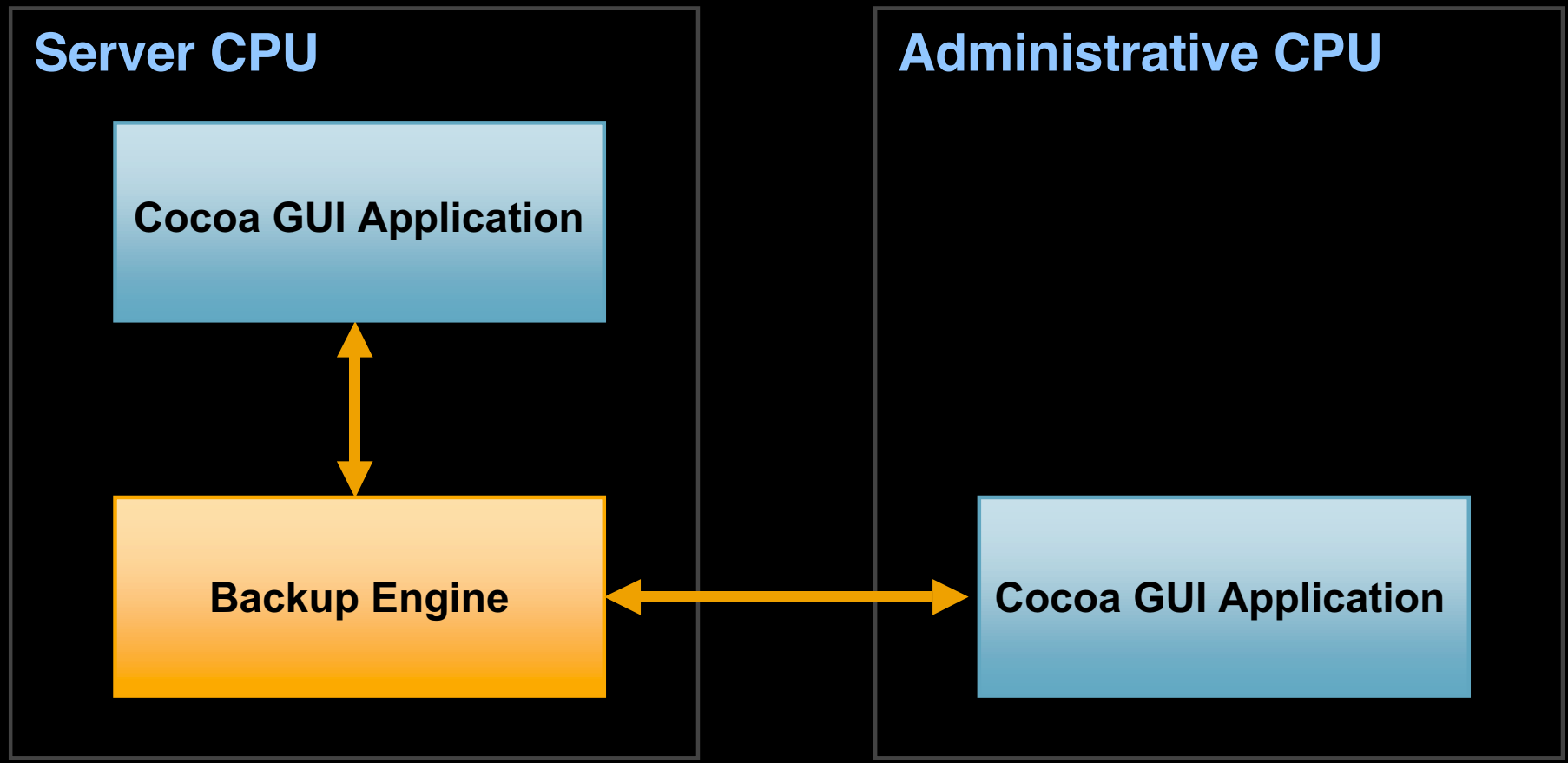
# Remote Server Administration




# Remote Server Administration




# Remote Server Administration



# Remote Server Administration

## Finding target server

- May want to provide server browser UI
- Use new DNS Service Discovery API to register and locate remote server
- Session 811 Zero Configuration Networking: Thurs., 2:00pm, Room J

# Remote Server Administration

- Package them in separate installers

Server Installer

Admin Installer

**Server CPU**

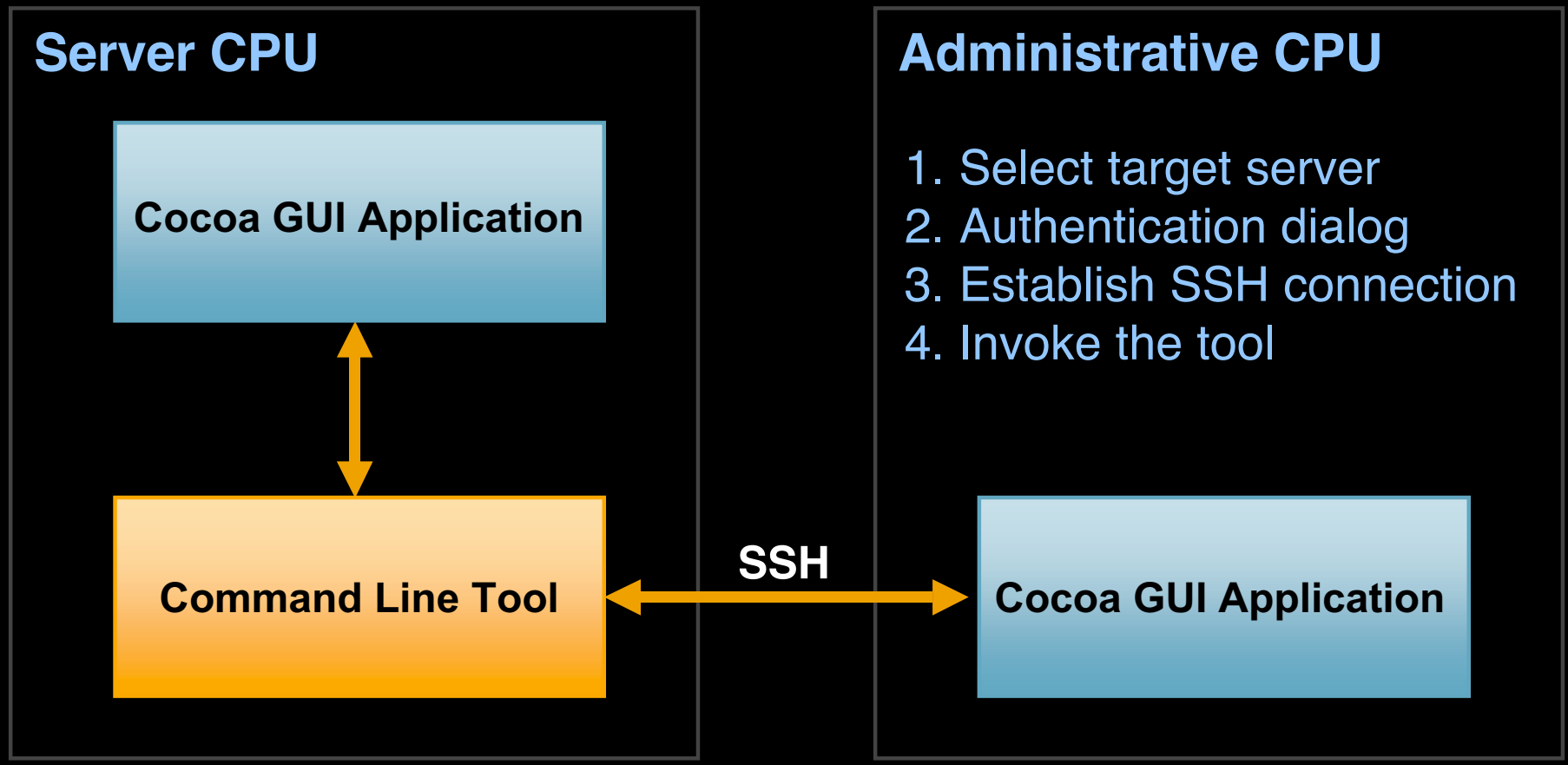
Backup Engine

**Administrative CPU**

Cocoa GUI Application

# Remote Server Administration

## Example: NetInfo Domain Setup




# Remote Server Monitoring

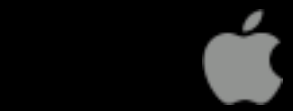
## Monitoring remote Jaguar Servers

- Terminal/SSH/command line tools

# Remote Server Monitoring

## Monitoring remote Jaguar Servers

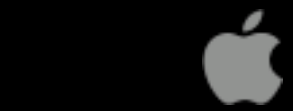
- Terminal/SSH/command line tools
- SNMP
  - NetSNMP ported and built into Jaguar desktop and server releases
  - Agent and basic MIBs
  - Compatiblity with industry standard tools



# Remote Server Monitoring

## Monitoring remote Jaguar Servers

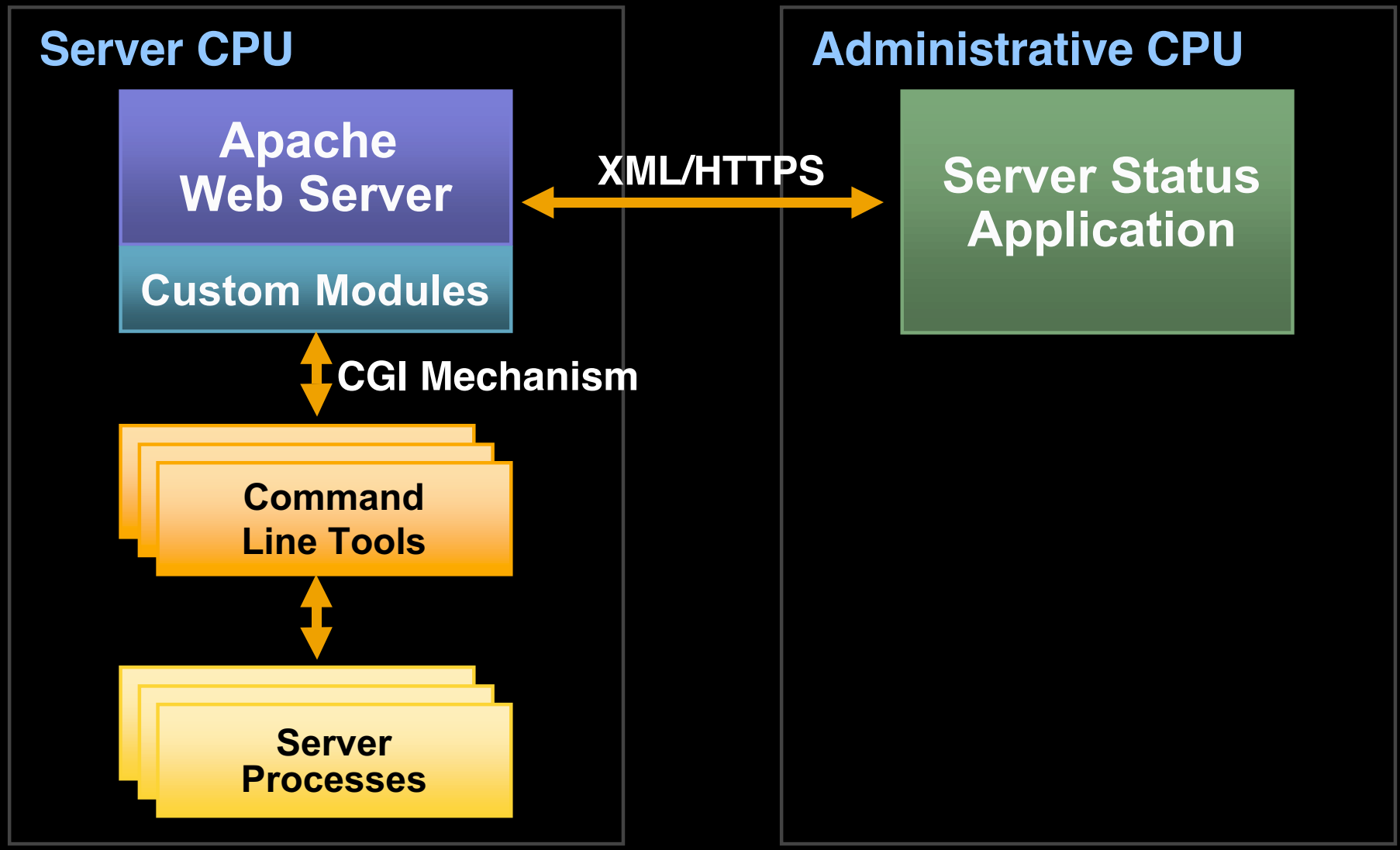
- Terminal/SSH/command line tools
- SNMP
    - NetSNMP ported and built into Jaguar desktop and server releases
    - Agent and basic MIBs
    - Compatiblity with industry standard tools
- New “Server Status” application



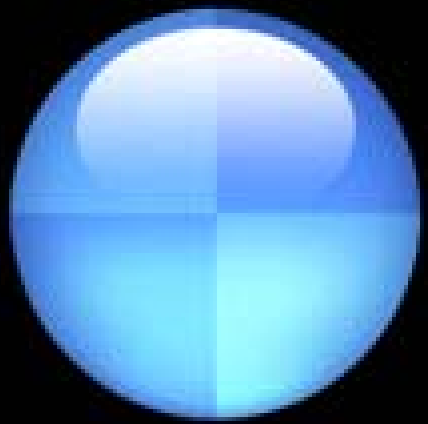
# Demo

## Server Status Application

# Server Status Architecture



# Open Directory



# Open Directory

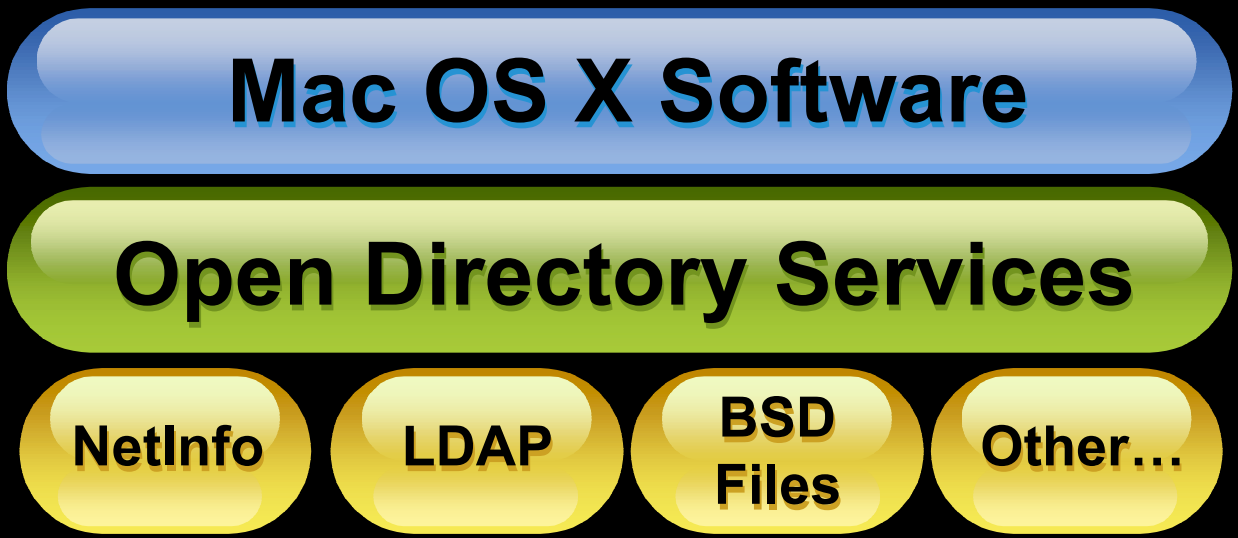
## What is it?

- Apple's standards-based directory services architecture
- Allows applications to share information about users and network resources
- Utilized by various components of Mac OS X Server and desktop
- New Password Server provides network authentication services

# Open Directory

**Standards-based directory services architecture**

- Read/write API
- API to create custom plug-ins
- And much more!



# Open Directory

## What information to store?

- User attributes
- Machine attributes
- Any shared information
- Service preferences
- . . .

# Open Directory

## What information should I store?

- User attributes
- Machine attributes
- Any shared information
- Service preferences
- . . .

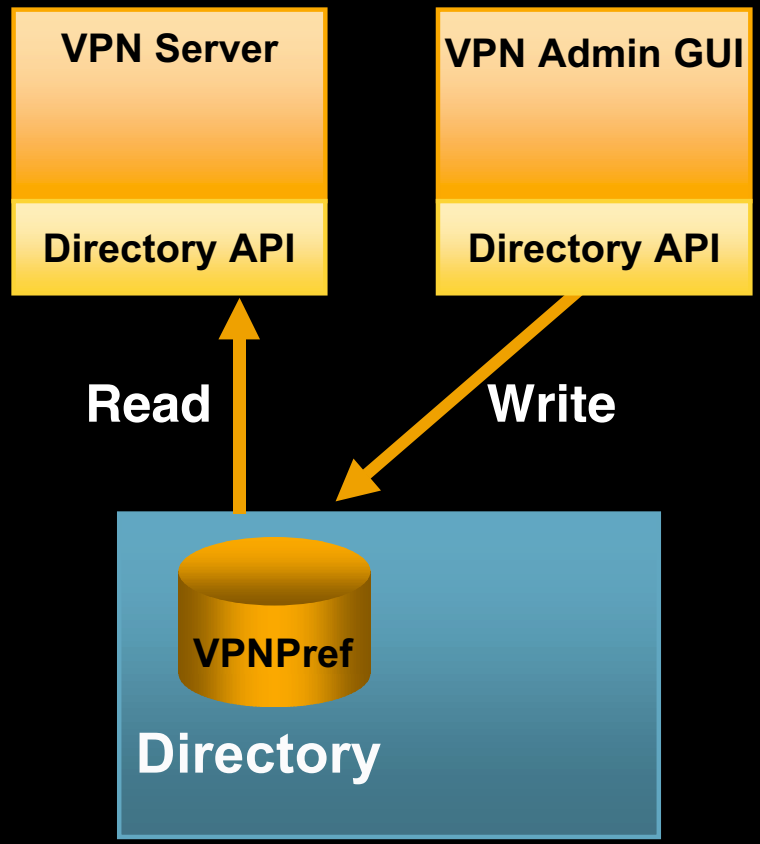
**User Record**

| | |
|---|---|
| name: | kazu |
| passwd: | xxxxxxxx |
| gid: | 20 |
| home: | /Users/kazu |
| shell: | /bin/tcsh |
| … | |
| vpn_quota: | 2 |

# Open Directory

## What information should I store?

- User attributes
- Machine attributes
- Any shared information
- Service preferences
- . . .




# Open Directory

## Password Server

- Based on SASL (Simple Authentication and Security Layer) standard
- Verifies password but no network password recovery
- Supports NT/LAN Manager, APOP, CRAM-MD5, SHA-1, and other popular authentication methods
- Password policy features
  - Disable account after a certain date
  - Enforce minimum password length
  - And more

# For More Information

**Open Directory**

- Session
  **813 Directory Services, Thu, 3:30pm, Room C**
- Online resources
  **developer.apple.com/techpubs/**
  **developer.apple.com/darwin/projects/opendirectory/**

# High Availability Services

**Scott Mulligan**
**Manager**
**Server Infrastructure Group**

# High Availability

Servers and services
that are always functioning
and available.

# High Availability

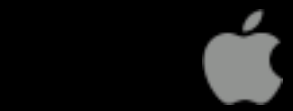
## Added reliability with Watchdog

- First introduced in Mac OS X Server 10.1
- Restarts crashed services
- Heartbeat restart
- For details: **$ man watchdog**

# High Availability

## New: Disk Space Monitor

- Introduced: today
- Configurable cron job periodically checks for volumes short on disk space
- Configurable alert script notifies administrator when first threshold is exceeded
- Configurable recovery script takes pre-determined actions when second threshold is exceeded



# High Availability

## Disk Space Monitor

- Default recovery actions include:
  - Compression of log files
  - Deletion of log files
- For details: **$ man diskspacemonitor**

# High Availability

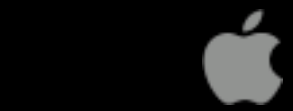
## New: IP Fail-Over Mechanism

- Introduced: today
- Stand-by server can take over primary server's network address if the primary server fails
- "Fail-back" when primary server returns
- Sends email notifications for all transitions
- Performs multiple ordered actions, before and after acquiring or relinquishing a network address

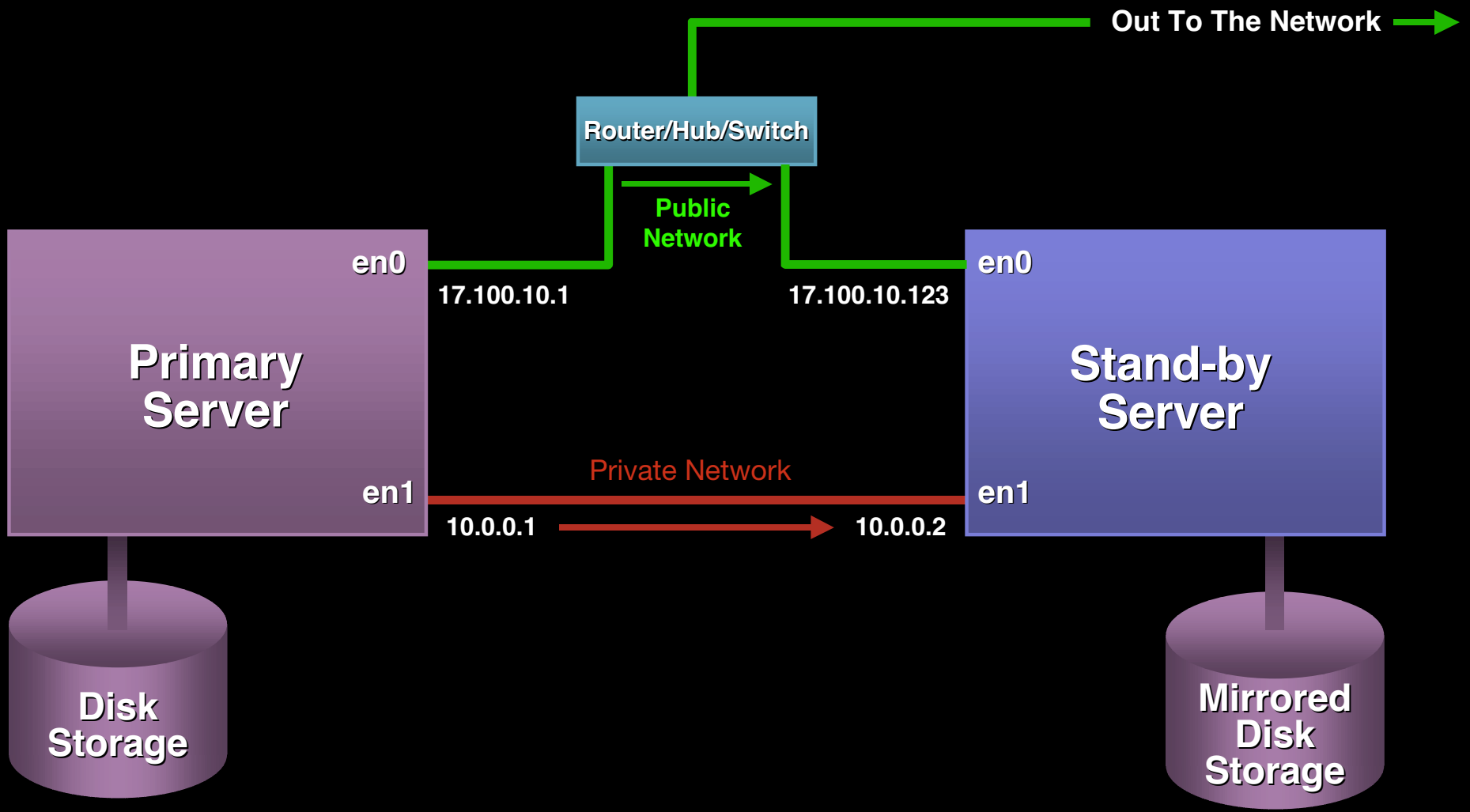
# High Availability

## IP Fail-Over Mechanism

- Services are notified of network transitions through standard OS mechanisms
- Option for notifications without fail-over
- Developer or customer extensible
- Simple and flexible
- Excellent solution for certain scenarios
- One component of a complete solution



# IP Fail-over


Out To The Network
Router/Hub/Switch
Public Network
en0
17.100.10.1
17.100.10.123
en0
Primary Server
Stand-by Server
Private Network
en1
10.0.0.1
10.0.0.2
en1
Disk Storage
Mirrored Disk Storage

# IP Fail-over

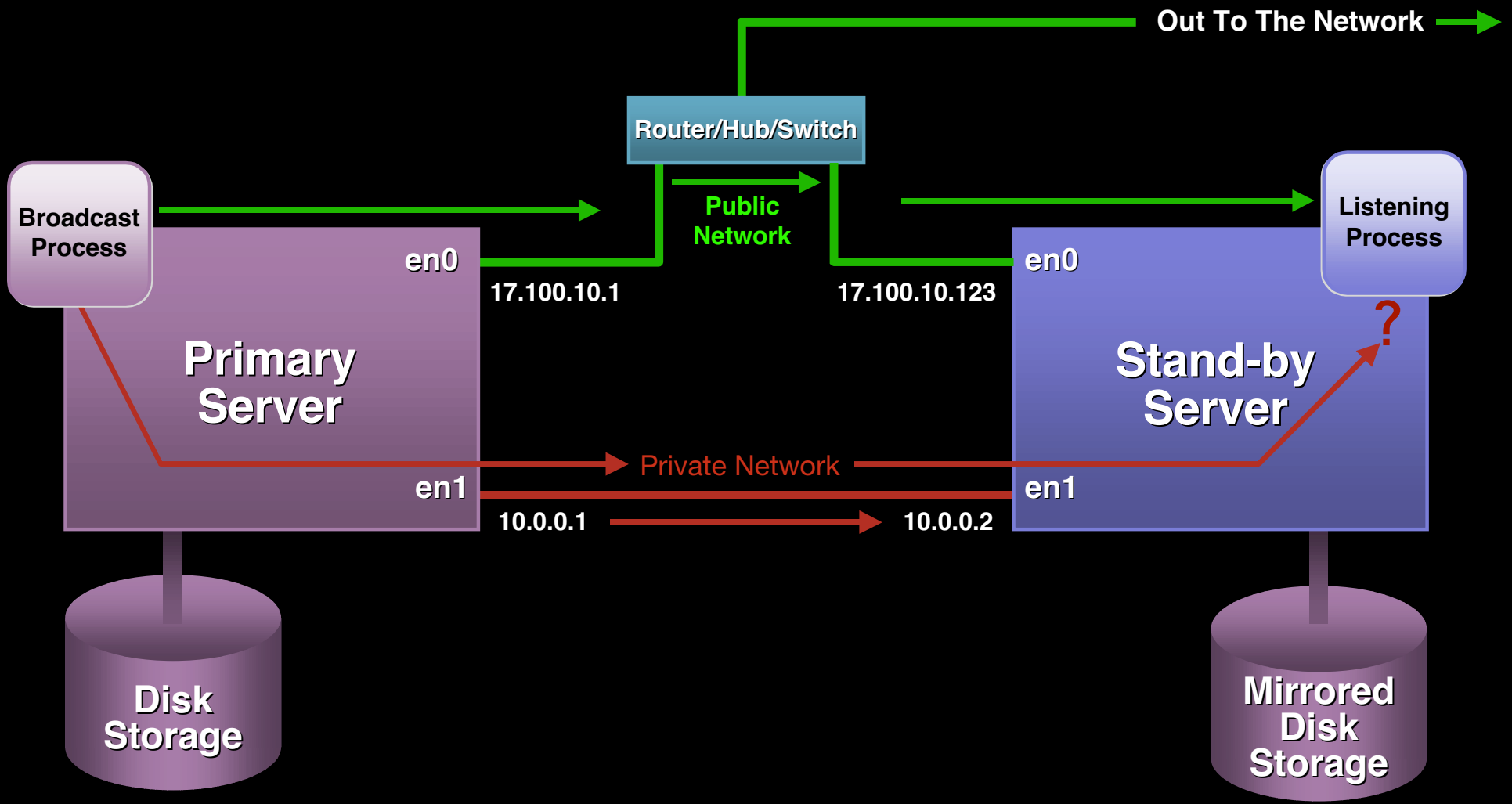
## Primary Server

- Has a well known address
- Has a less known address
- Broadcasts “I’m here!”

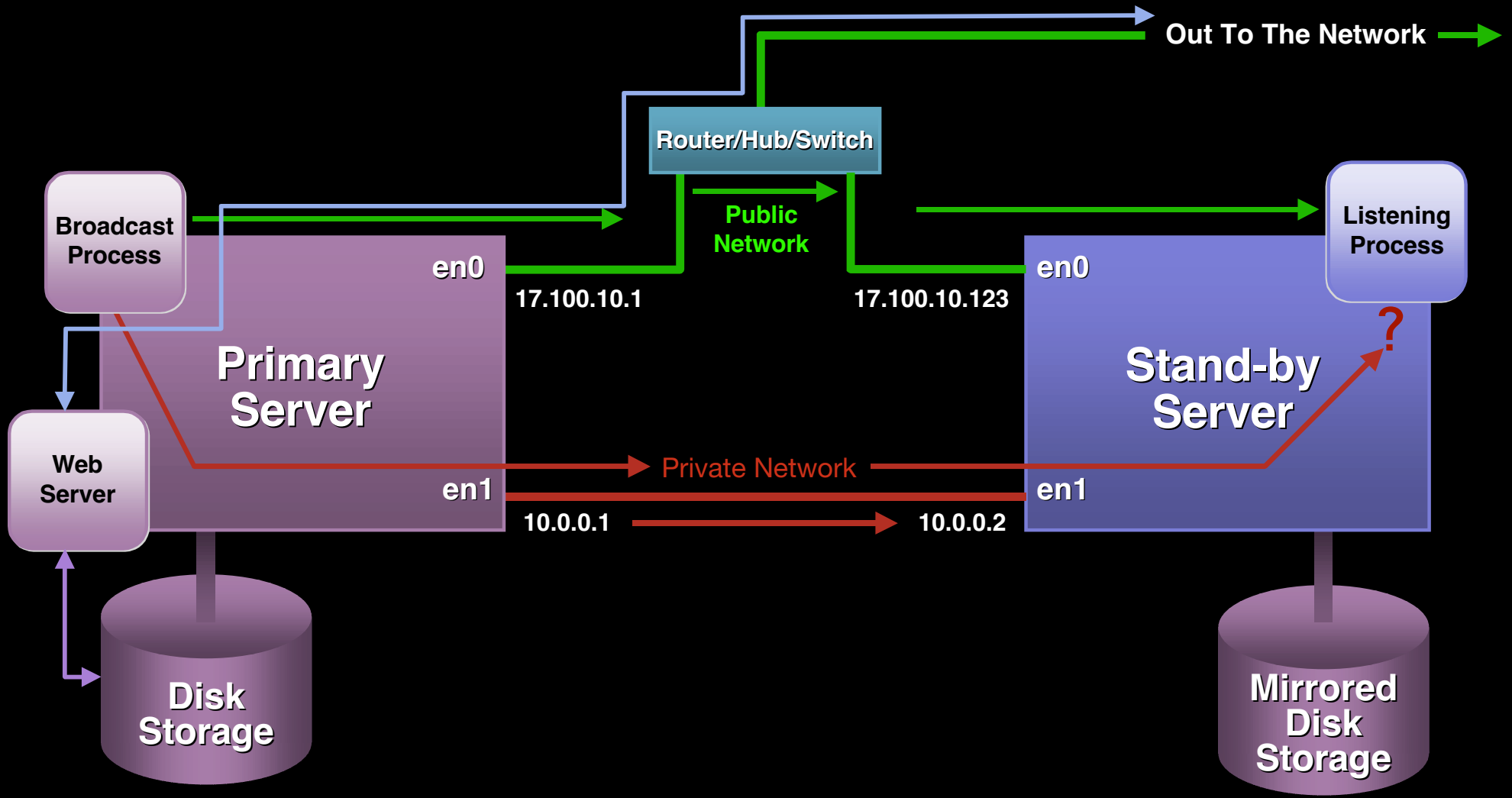
## Stand-by Server

- Has a well known address
- Has a less known address
- Listens for primary server

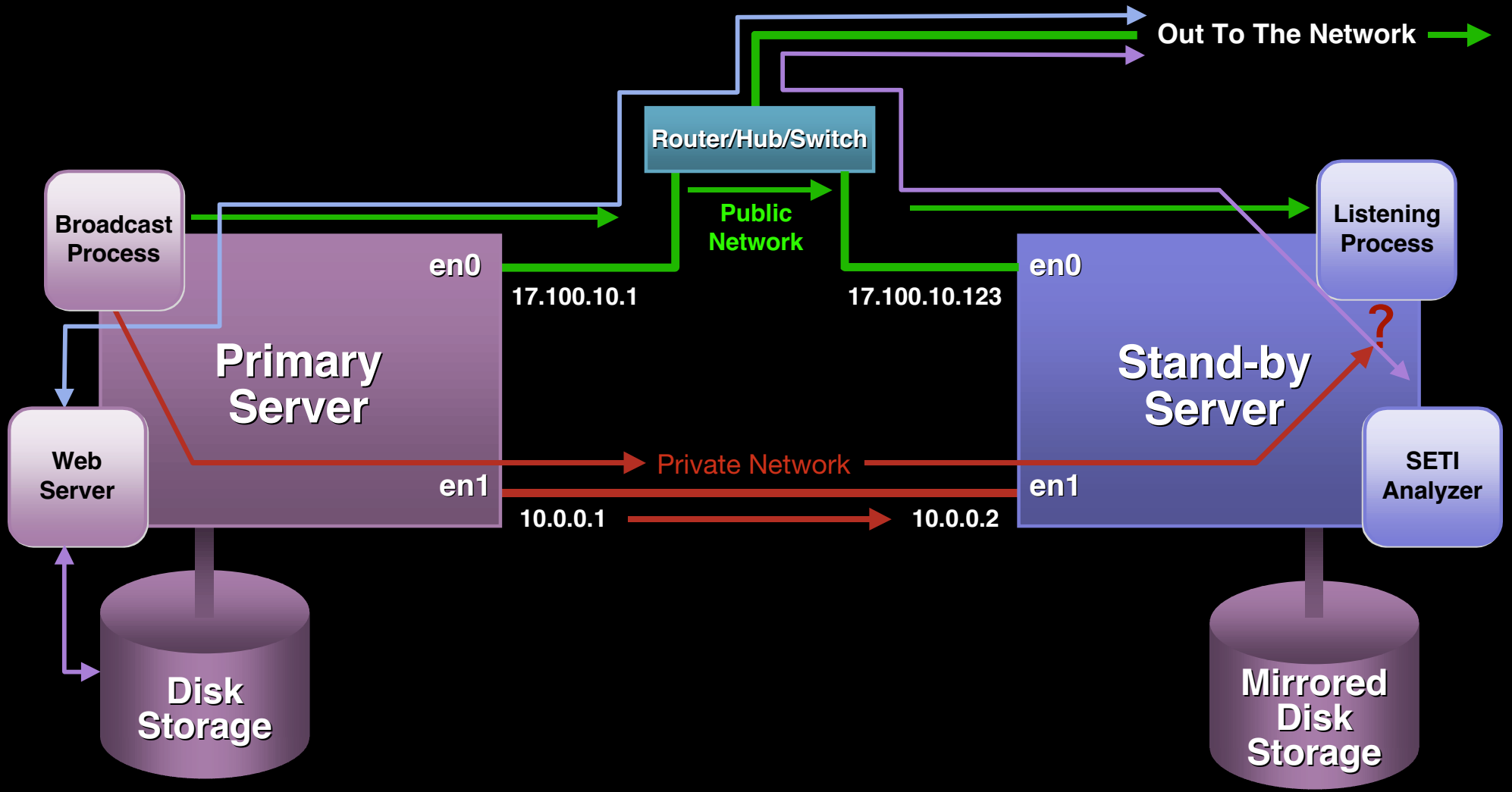
# IP Fail-over


Out To The Network
Router/Hub/Switch
Broadcast Process
Public Network
Listening Process
en0
17.100.10.1
17.100.10.123
en0
Primary Server
Stand-by Server
?
Private Network
en1
en1
10.0.0.1
10.0.0.2
Disk Storage
Mirrored Disk Storage

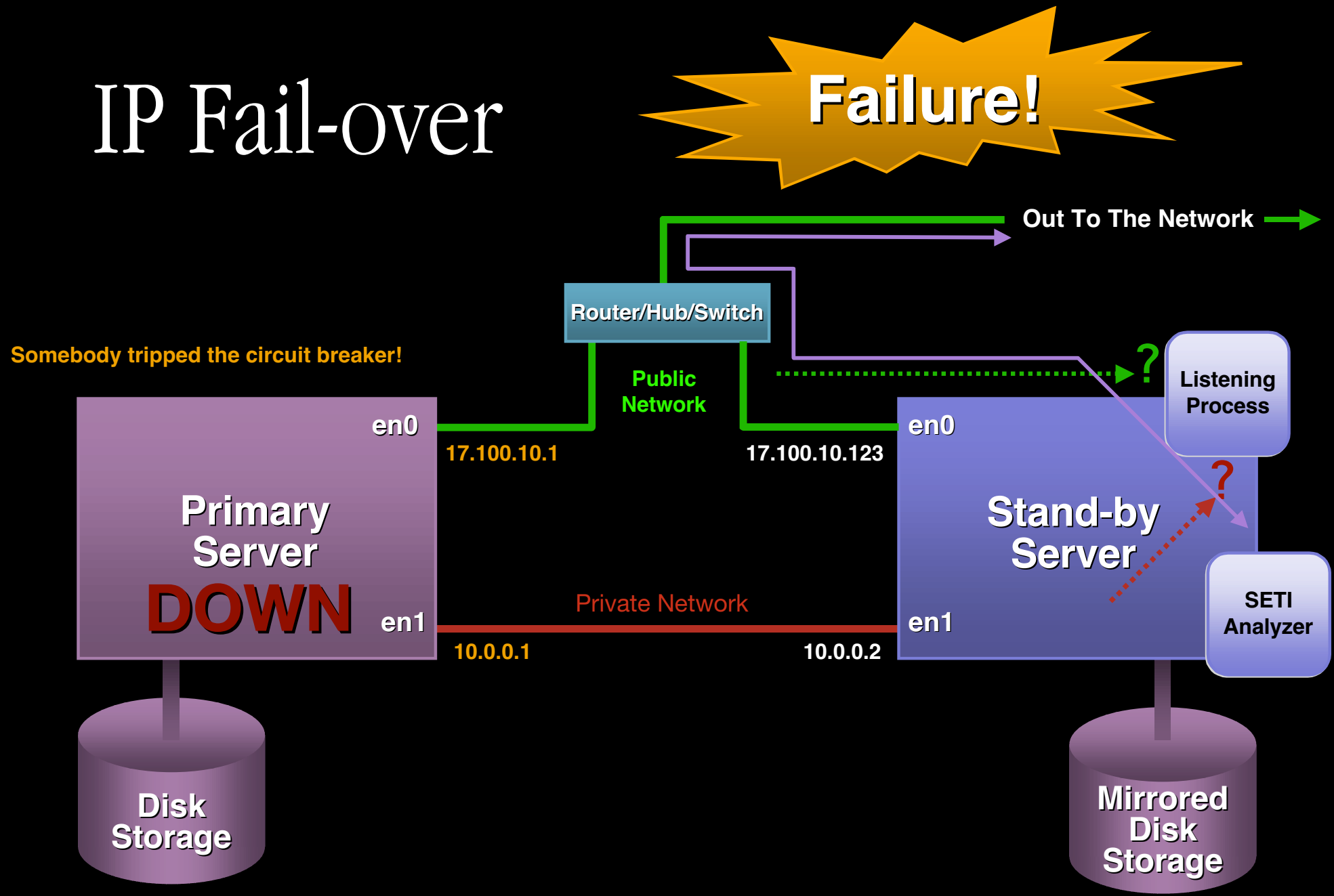
# IP Fail-over


Out To The Network
Router/Hub/Switch
Broadcast Process
Public Network
Listening Process
en0
17.100.10.1
17.100.10.123
en0
Primary Server
Stand-by Server
?
Web Server
Private Network
en1
en1
10.0.0.1
10.0.0.2
Disk Storage
Mirrored Disk Storage

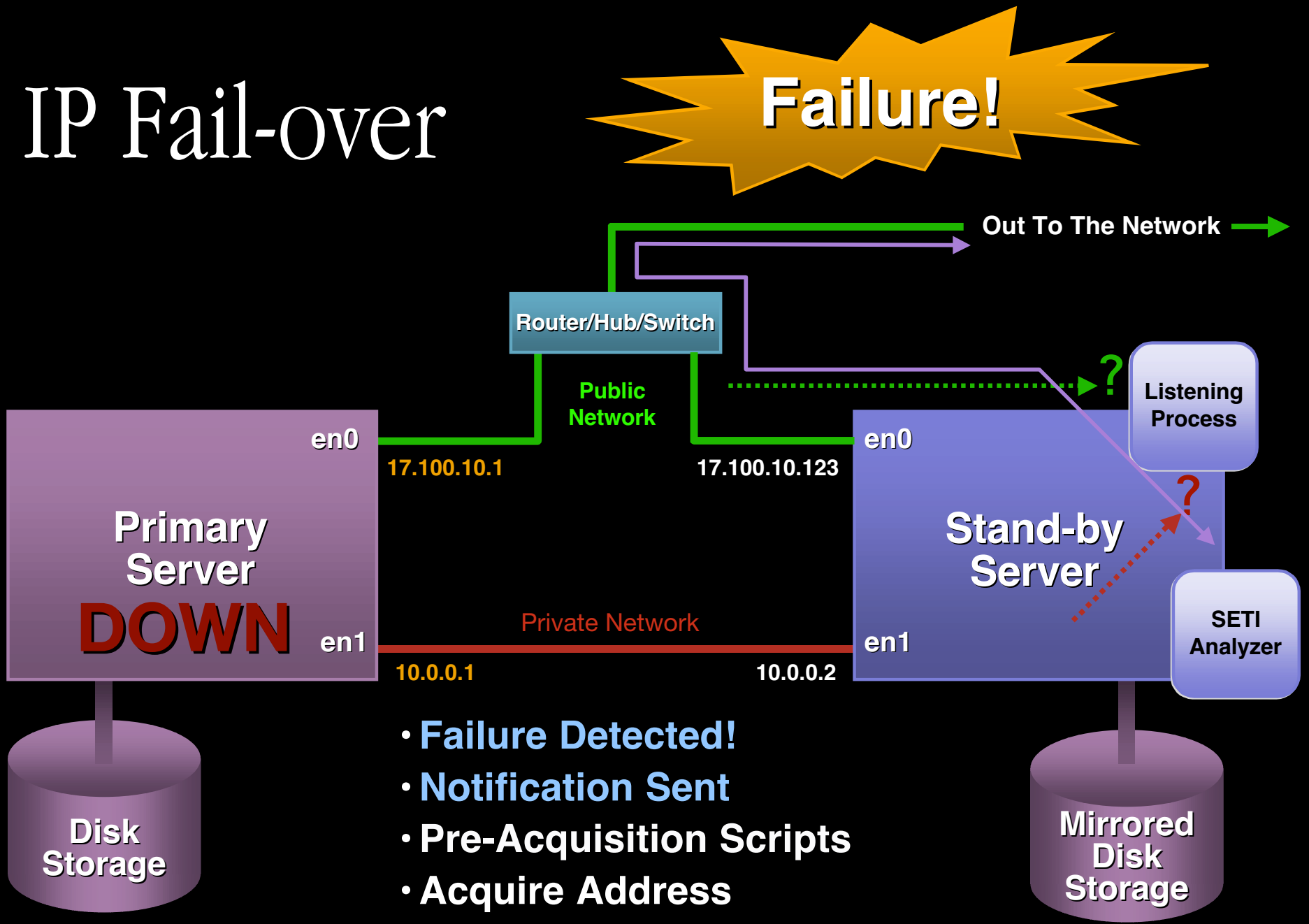
# IP Fail-over


Out To The Network
Router/Hub/Switch
Broadcast Process
Public Network
Listening Process
en0
17.100.10.1
17.100.10.123
en0
Primary Server
Stand-by Server
?
Web Server
Private Network
en1
en1
SETI Analyzer
10.0.0.1
10.0.0.2
Disk Storage
Mirrored Disk Storage

# IP Fail-over

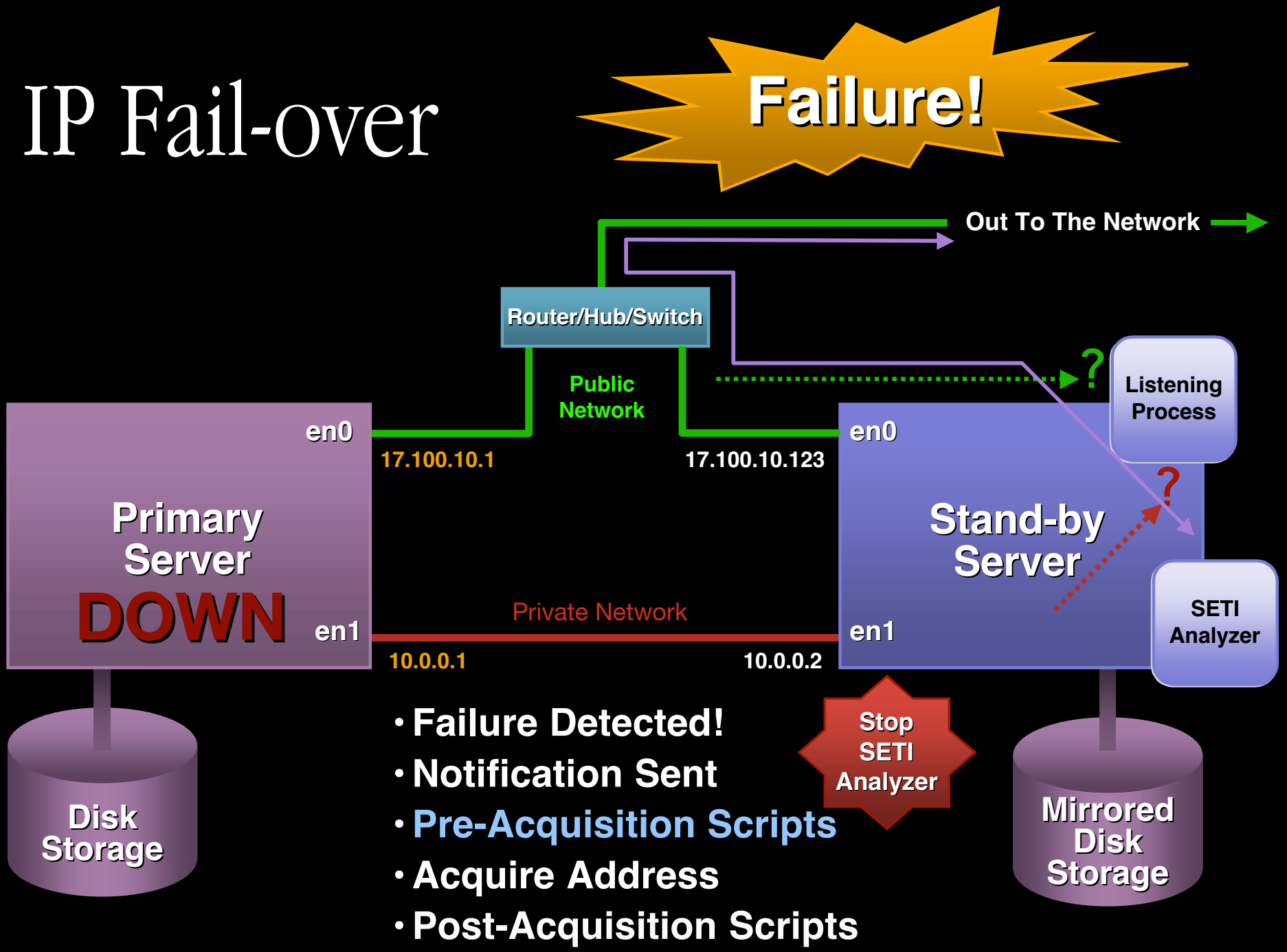

Failure!
Out To The Network
Router/Hub/Switch
Somebody tripped the circuit breaker!
Public Network
?
Listening Process
en0
17.100.10.1
17.100.10.123
en0
Primary Server
DOWN
Stand-by Server
?
SETI Analyzer
Private Network
en1
en1
10.0.0.1
10.0.0.2
Disk Storage
Mirrored Disk Storage

# IP Fail-over



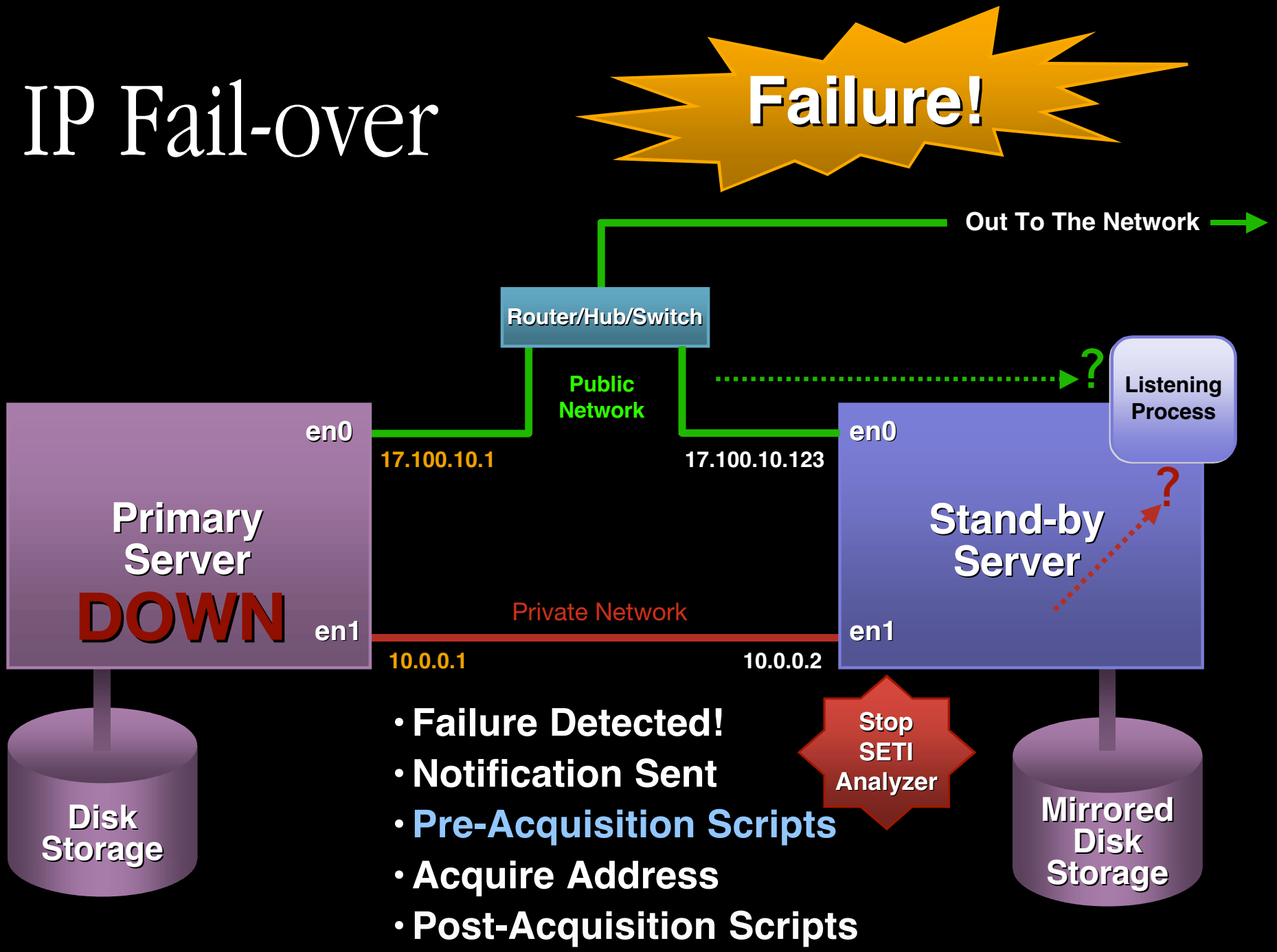

- Failure Detected!
- Notification Sent
- Pre-Acquisition Scripts
- Acquire Address
- Post-Acquisition Scripts

# IP Fail-over

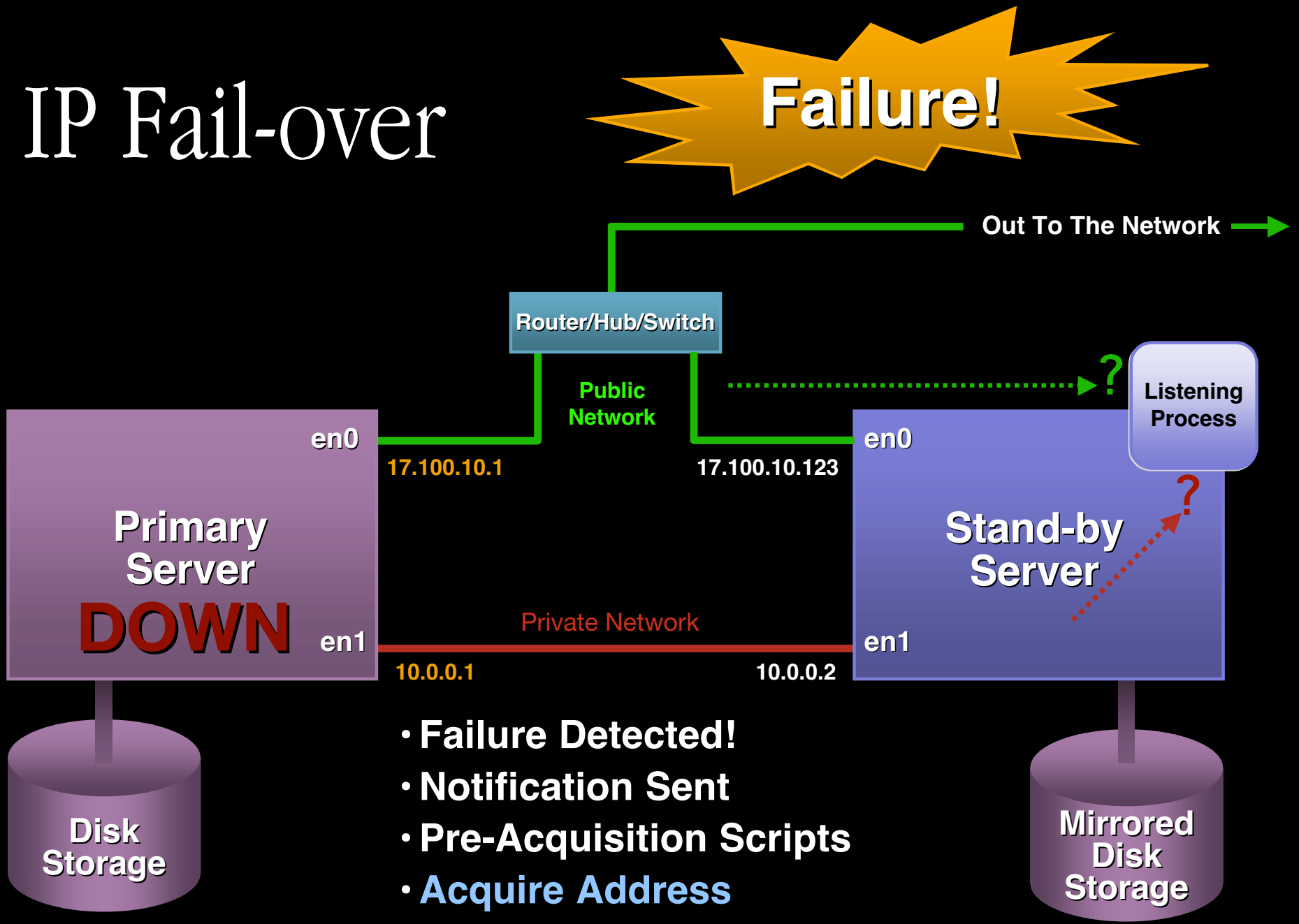



- Failure Detected!
- Notification Sent
- Pre-Acquisition Scripts
- Acquire Address
- Post-Acquisition Scripts

# IP Fail-over

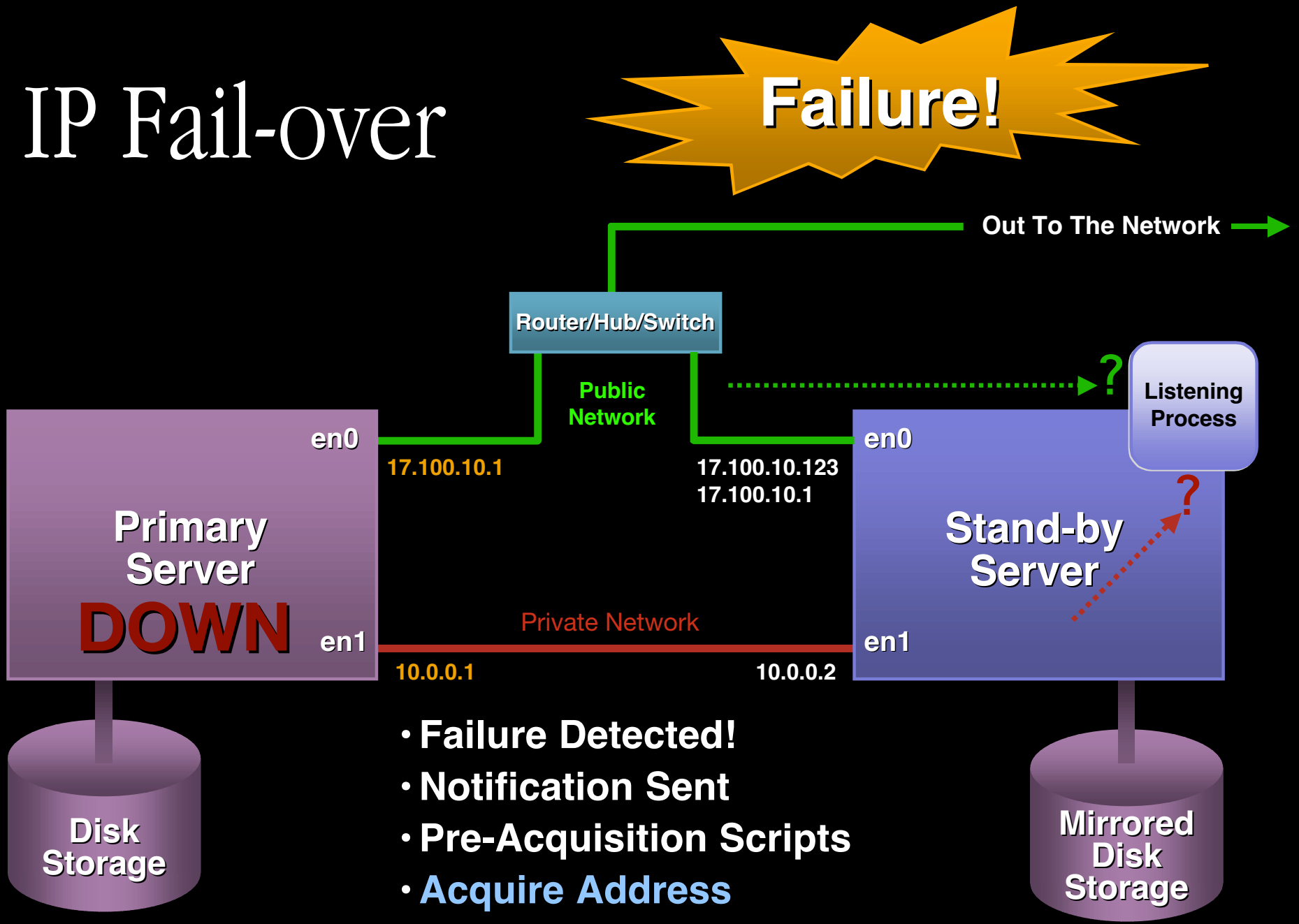

Failure!
Out To The Network
Router/Hub/Switch
Public Network
?
Listening Process
en0
17.100.10.1
17.100.10.123
en0
Primary Server
DOWN
en1
Private Network
10.0.0.1
10.0.0.2
en1
?
Stand-by Server
Stop SETI Analyzer
Disk Storage
Mirrored Disk Storage
• Failure Detected!
• Notification Sent
• Pre-Acquisition Scripts
• Acquire Address
• Post-Acquisition Scripts

# IP Fail-over



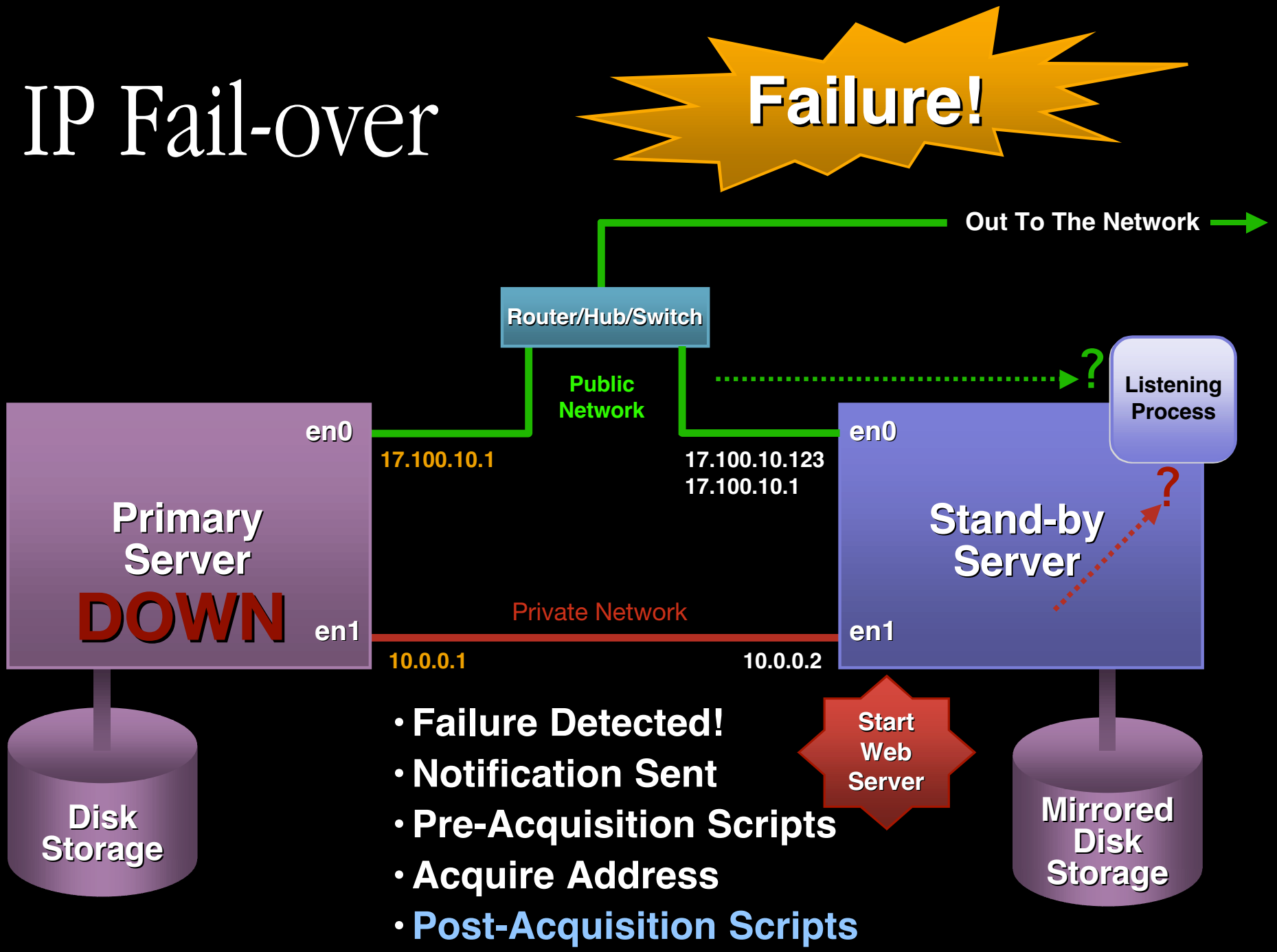

- Failure Detected!
- Notification Sent
- Pre-Acquisition Scripts
- Acquire Address
- Post-Acquisition Scripts

# IP Fail-over

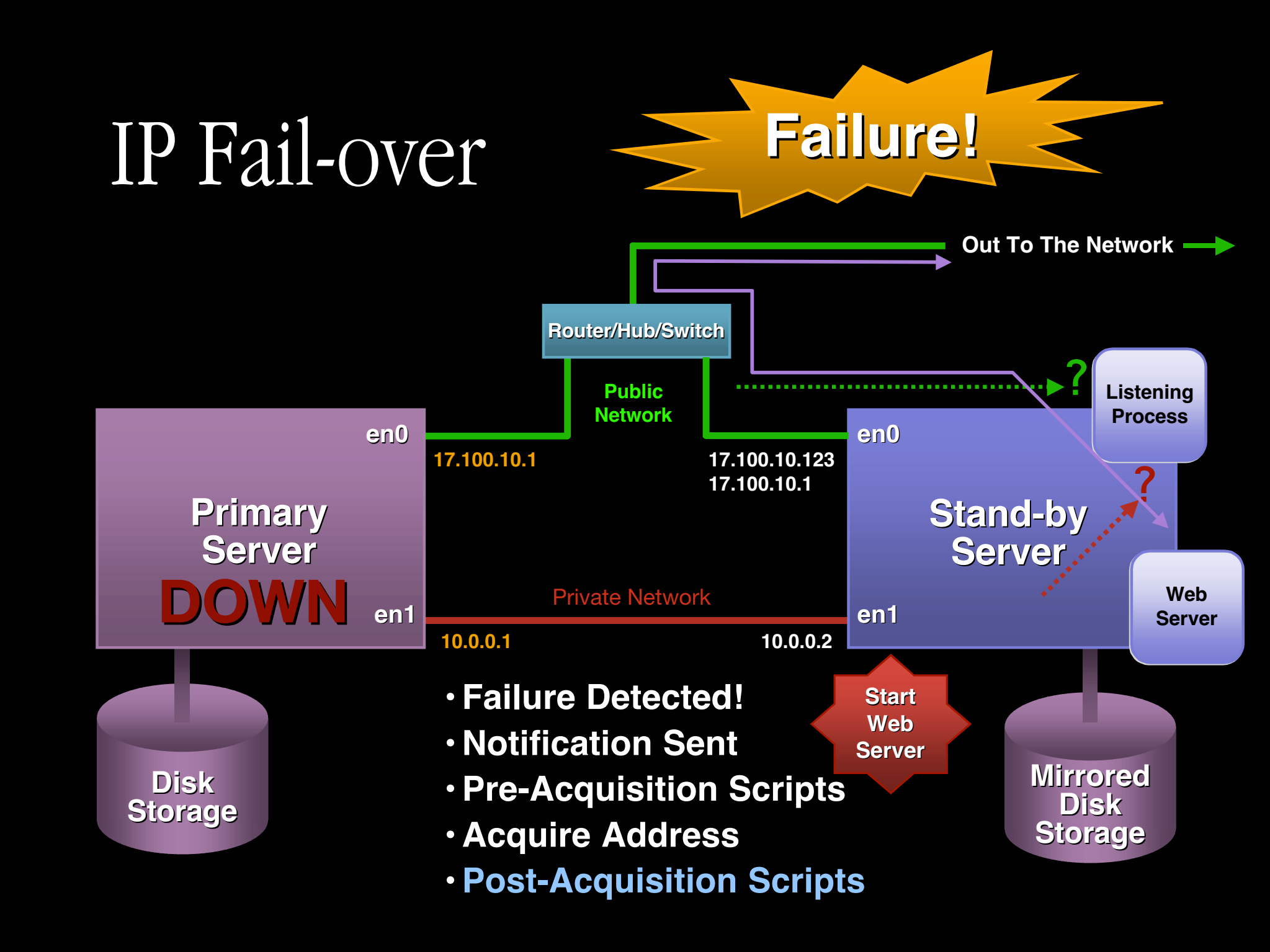



- Failure Detected!
- Notification Sent
- Pre-Acquisition Scripts
- Acquire Address
- Post-Acquisition Scripts

# IP Fail-over

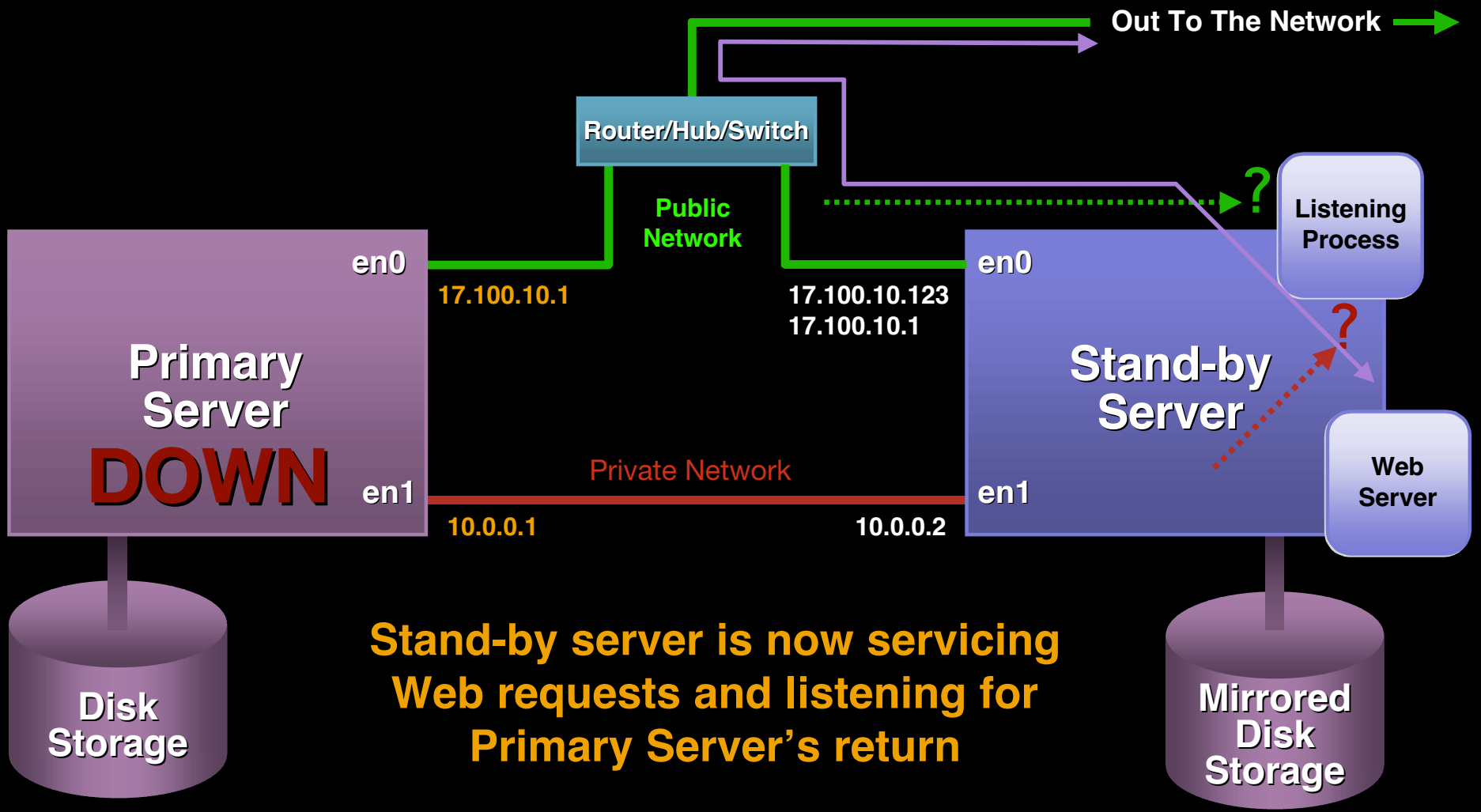

Failure!
Out To The Network
Router/Hub/Switch
Public Network
?
Listening Process
en0
17.100.10.1
17.100.10.123
17.100.10.1
en0
Primary Server
DOWN
en1
Private Network
Stand-by Server
?
en1
10.0.0.1
10.0.0.2
Start Web Server
Disk Storage
Mirrored Disk Storage
• Failure Detected!
• Notification Sent
• Pre-Acquisition Scripts
• Acquire Address
• Post-Acquisition Scripts

# IP Fail-over




- Failure Detected!
- Notification Sent
- Pre-Acquisition Scripts
- Acquire Address
- Post-Acquisition Scripts

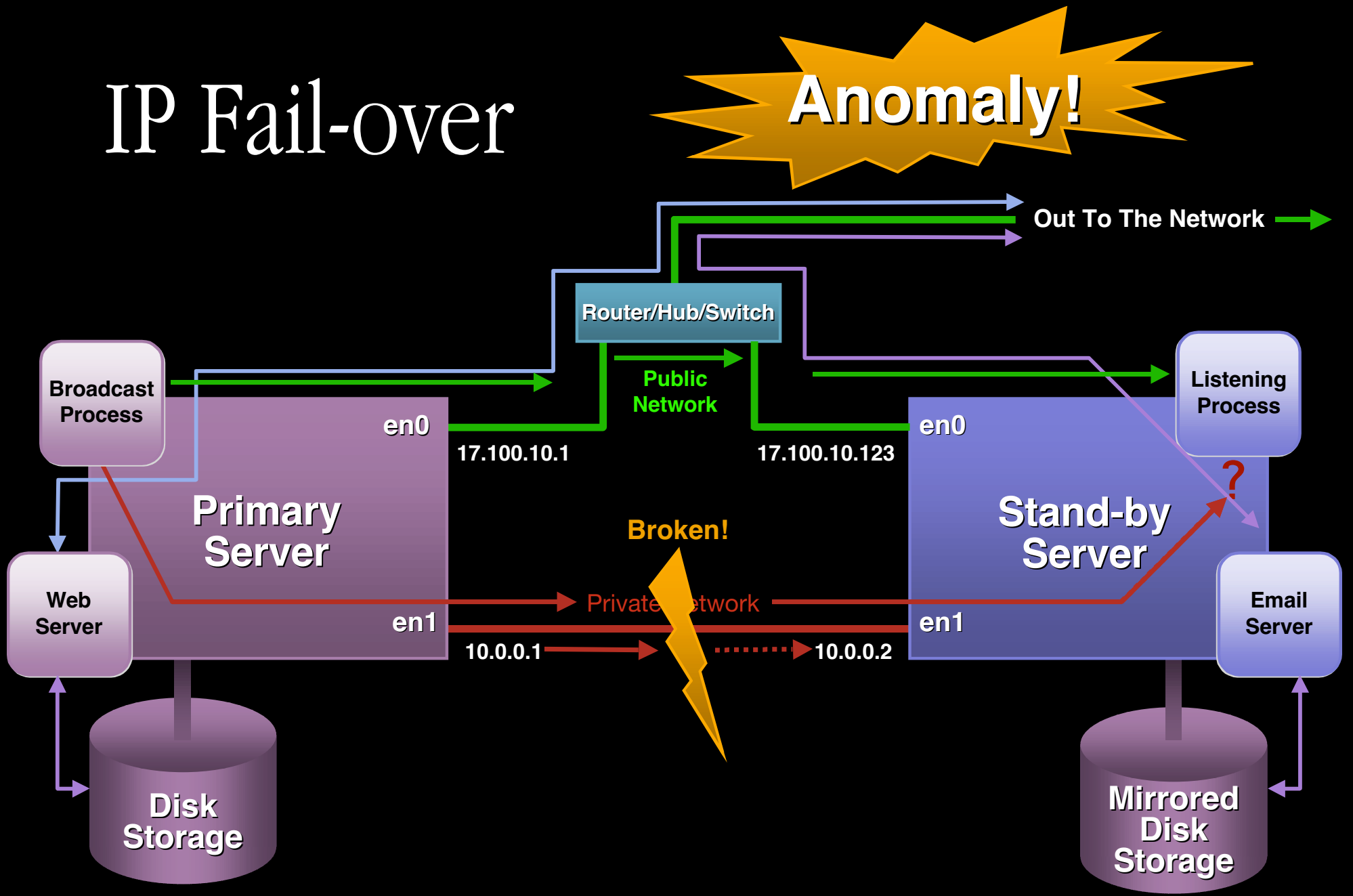
# IP Fail-over


Out To The Network
Router/Hub/Switch
Public Network
?
Listening Process
en0
17.100.10.1
17.100.10.123
17.100.10.1
en0
Primary Server
DOWN
en1
Private Network
Stand-by Server
?
Web Server
en1
10.0.0.1
10.0.0.2
Disk Storage
Stand-by server is now servicing Web requests and listening for Primary Server's return
Mirrored Disk Storage

# IP Fail-over

- Primary server is determined to be down when broadcast packets are missing from both the public and private networks
- An absence of broadcast packets on only one network is considered an anomaly. Anomalies will trigger notifications to be sent, but will not trigger a fail-over action

# IP Fail-over


Anomaly!
Out To The Network
Router/Hub/Switch
Broadcast Process
Public Network
Listening Process
en0
17.100.10.1
17.100.10.123
en0
Primary Server
Broken!
Stand-by Server
?
Web Server
Private Network
en1
en1
Email Server
10.0.0.1
10.0.0.2
Disk Storage
Mirrored Disk Storage

# IP Fail-over

- The private network is used to:
  - Verify primary server failure
  - Detect primary server recovery
- Anomalies:
  - Never cause the fail-over action
  - Always trigger the notification action
- Fail-back:
  - Works similarly to fail-over, with notifications and Pre- and Post- release extensibility

# IP Fail-over

- Components
  - The broadcast daemon process
  - The listener daemon process
  - Notification script
  - Sample scripts for Pre- and Post- address acquisition
  - Sample scripts for Pre- and Post- address relinquishment
  - Man pages

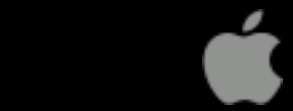
# File Services Update

**Rusty Tucker**
**Manager**
**File Services Group**

# File Services Update

## Security changes

- Kerberos v5 Support
  - AFP Client
  - AFP Server
  - FTP Server
- Kerberos v4 Support
  - In AFP Client for legacy compatibility
- AFP connection via SSH tunnel



# File Services Update

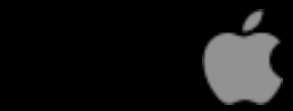
## AFP performance enhancements

- Read and write performance
  - Includes TCP stack changes in the kernel
- Scalability
  - AFP Server allocates and kills worker threads as needed
- Faster mount time (Connect To)
- Client Side Caching
  - Use “Read-only” access mode whenever possible

# File Services Update

## Other features

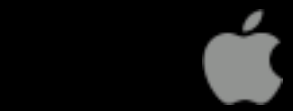
- BSD Quota support
  - EDQUOTA error mapping
  - Home directory quota limits
- Significantly enhanced sharing functionality
  - Brand new management UI
  - Per service share points
  - Custom share point names



# File Services Update

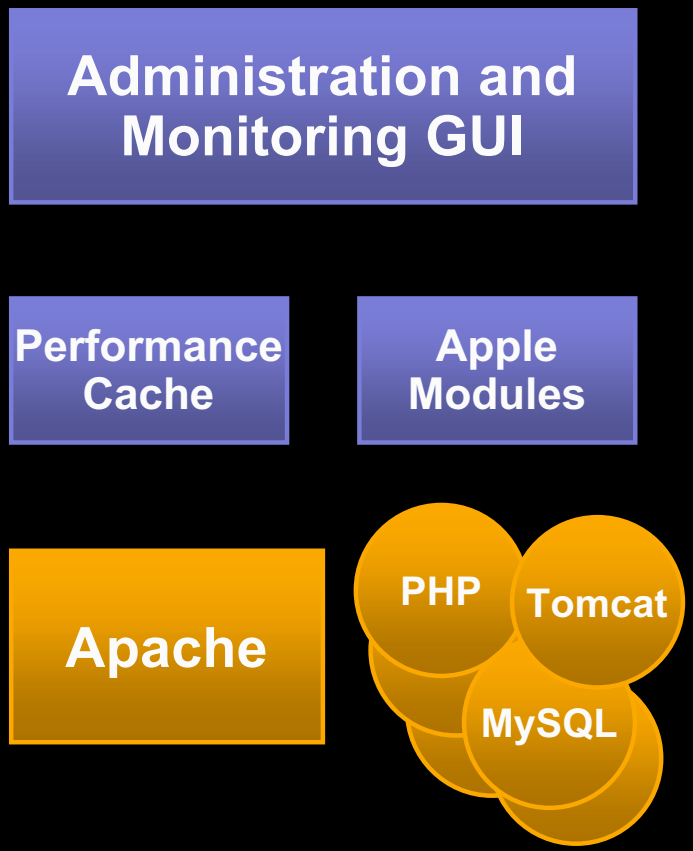
## AFP home directory features

- Automatic reconnect as needed
- Improved UNIX fidelity
    - No permission mapping for network users
    - AFP connections show true owner and group
    - Better “delete while open” compatibility
    - Symlink support
- Automatic home directory creation



# Web Platform

# Web Platform




- Apache
- Additional open source packages
- Apple additions
  - Performance cache
  - Custom modules
  - Admin and monitoring GUI

# Web Platform

## Great web application platform

- WebObjects—Top rated application server
- MySQL—multiuser SQL database
- PHP—‘C’ like scripting, database access
- Perl—text manipulation, database access
- Tomcat—Java Servlets, Java Server pages

# Web Platform

## And more!

- Fast Java platform
- Apache 2 also bundled
- Built-in media streaming server—QTSS
    - Streams live and stored media
    - QuickTime, MPEG-4, MP3 support
    - Playlist to simulate live broadcast

# Roadmap

| | |
|---|---|
| **813 Directory Services** | Room C<br>**Thurs., 3:30pm** |
| **812 QuickTime Streaming Server 4** | Civic<br>**Thurs., 2:00pm** |
| **815 Developing for the Managed Desktop** | Room J<br>**Fri., 9:00am** |
| **810 Customizing NetBoot and NetInstall** | Room J<br>**Thurs., 10:30am** |

# Roadmap

| | |
|---|---|
| **FF017 Feedback Forum: Server Services** | Room J<br>**Fri., 5:00pm** |
| **814 Kerberos in Mac OS X** | Room C<br>**Thurs., 5:00pm** |
| **811 Zero Configuration Networking** | Room J<br>**Thurs., 2:00pm** |

# Who to Contact

**Tom Weyer**
Network and Communications Evangelist
weyer@apple.com

http://developer.apple.com/wwdc2002/urls.html

# For More Information

- Mac OS X Server web sites

  **http://www.apple.com/macosx/server/**
  **http://www.apple.com/darwin/projects/streaming/**
  **http://www.apple.com/darwin/projects/opendirectory/**

- Apple Customer Training

  **http://train.apple.com/**

- Online developer documentation

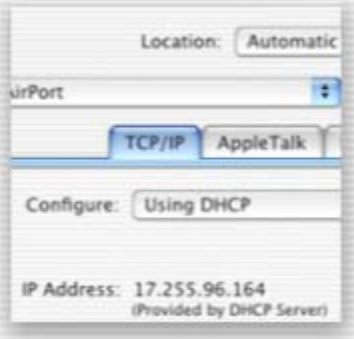
  **http://developer.apple.com/techpubs/macosx/**

- Mailing list

  **http://lists.apple.com/**

# Q&A






**Tom Weyer**
**Network and Communications Evangelist**
**weyer@apple.com**

**http://developer.apple.com/wwdc2002/urls.html**


WWDC2002


WWDC2002


WWDC2002